Emerging Threats and Trends

How To Social Engineer With 100% Success Using OSINT

Dave Marcus
Director
McAfee Labs

.

Agenda

- Social Engineering 101 and OSINT
- The Tools To Rule Them All
- Game Time!!!

Social Engineering 101

- What is Social Engineering?
- Why does Social Engineering work?
- When does Social Engineering NOT work?
- Can Social Engineering be done with near 100% success?
- Using OSINT

What is OSINT?

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or classified sources); it is not related to open-source software or public intelligence.

Wikipedia Definition

Forms of OSINT

OSINT includes a wide variety of information and sources:

* Media: newspapers, magazines, radio, television, and computer-based information.

* Web-based communities and user generated content: social-networking sites, video sharing sites, wikis, blogs, and folksonomies.

* Public data: government reports, official data such as budgets, demographics, hearings, legislative debates, press conferences, speeches, marine and aeronautical safety warnings, environmental impact statements and contract awards.

* Observation and reporting: amateur airplane spotters, radio monitors and satellite observers among many others have provided significant information not otherwise available. The availability of worldwide satellite photography, often of high resolution, on the Web (e.g., Google Earth) has expanded open source capabilities into areas formerly available only to major intelligence services.

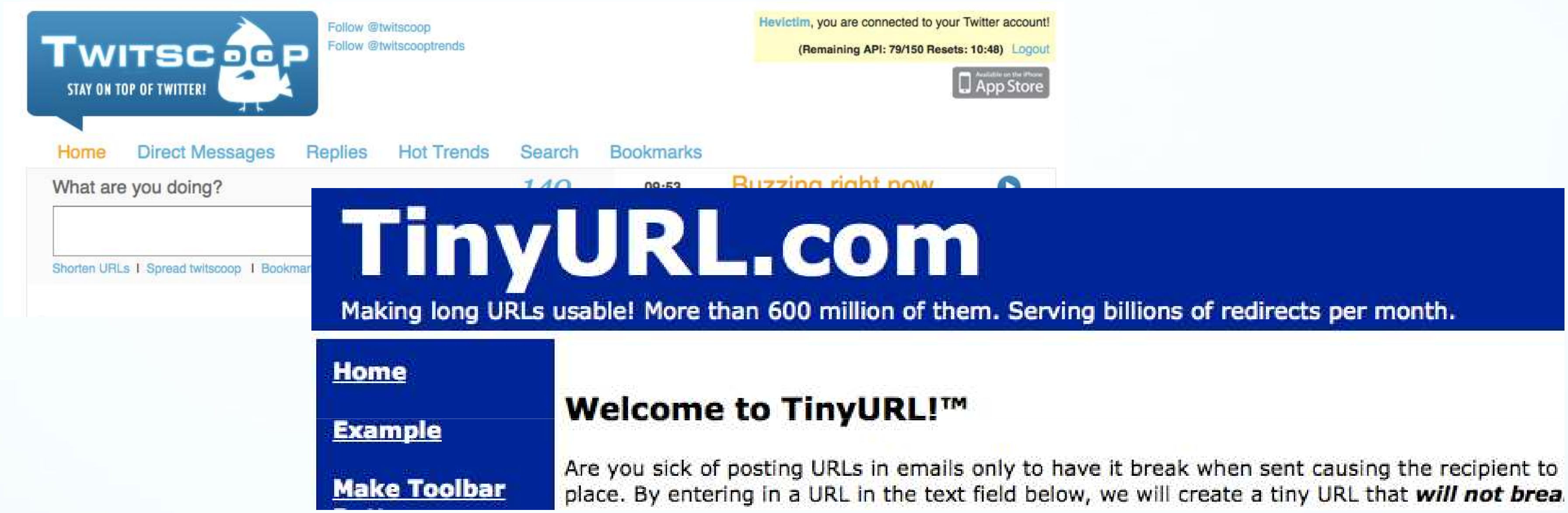
* Professional and academic: conferences, symposia, professional associations, academic papers, and subject matter experts.

Wikipedia Definition

Our Needed OSINT Toolset

- We need a tool to mine the data, trends and topics that our victims are CURRENTLY talking about
- We need a tool to DELIVER stuff…..
- We need a tool that HIDES our true intentions
- We need a tool that CREATES naughty bits!!
- We need these tools for FREE

Enter Social Networking



Follow @twitscoop
Follow @twitscooptrends

Hevictim, you are connected to your Twitter account!
(Remaining API: 79/150 Resets: 10:48) Logout

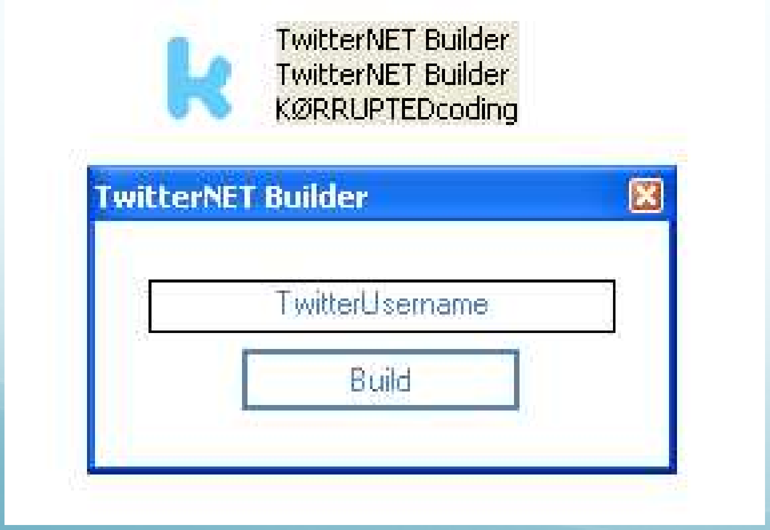
What are you doing?

TinyURL.com

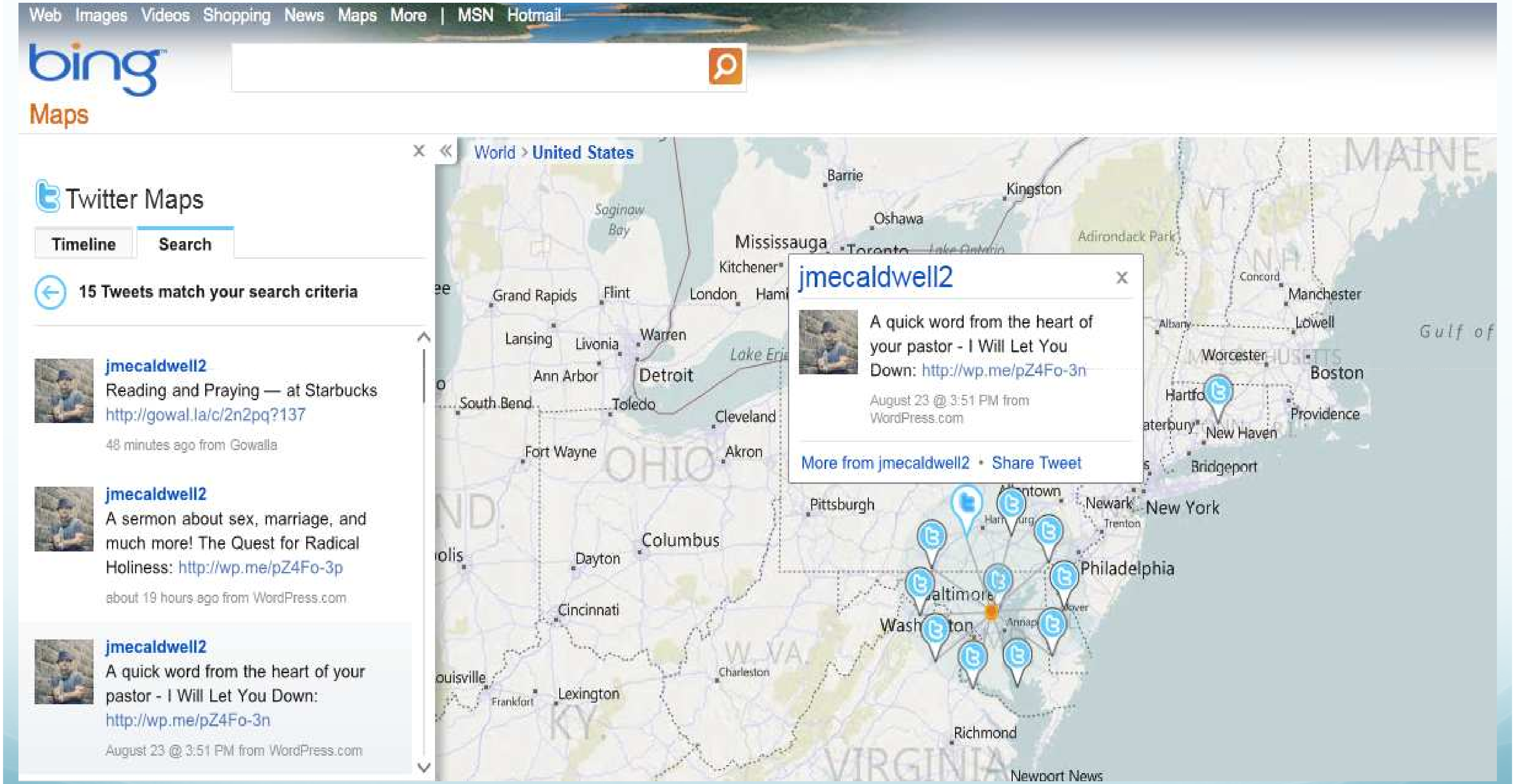
Making long URLs usable! More than 600 million of them. Serving billions of redirects per month.

Welcome to TinyURL!™

Are you sick of posting URLs in emails only to have it break when sent causing the recipient to
place. By entering in a URL in the text field below, we will create a tiny URL that ***will not brea***


TwitterNET Builder
TwitterNET Builder
KØRRUPTEDcoding

Mining Bing



15 Tweets match your search criteria

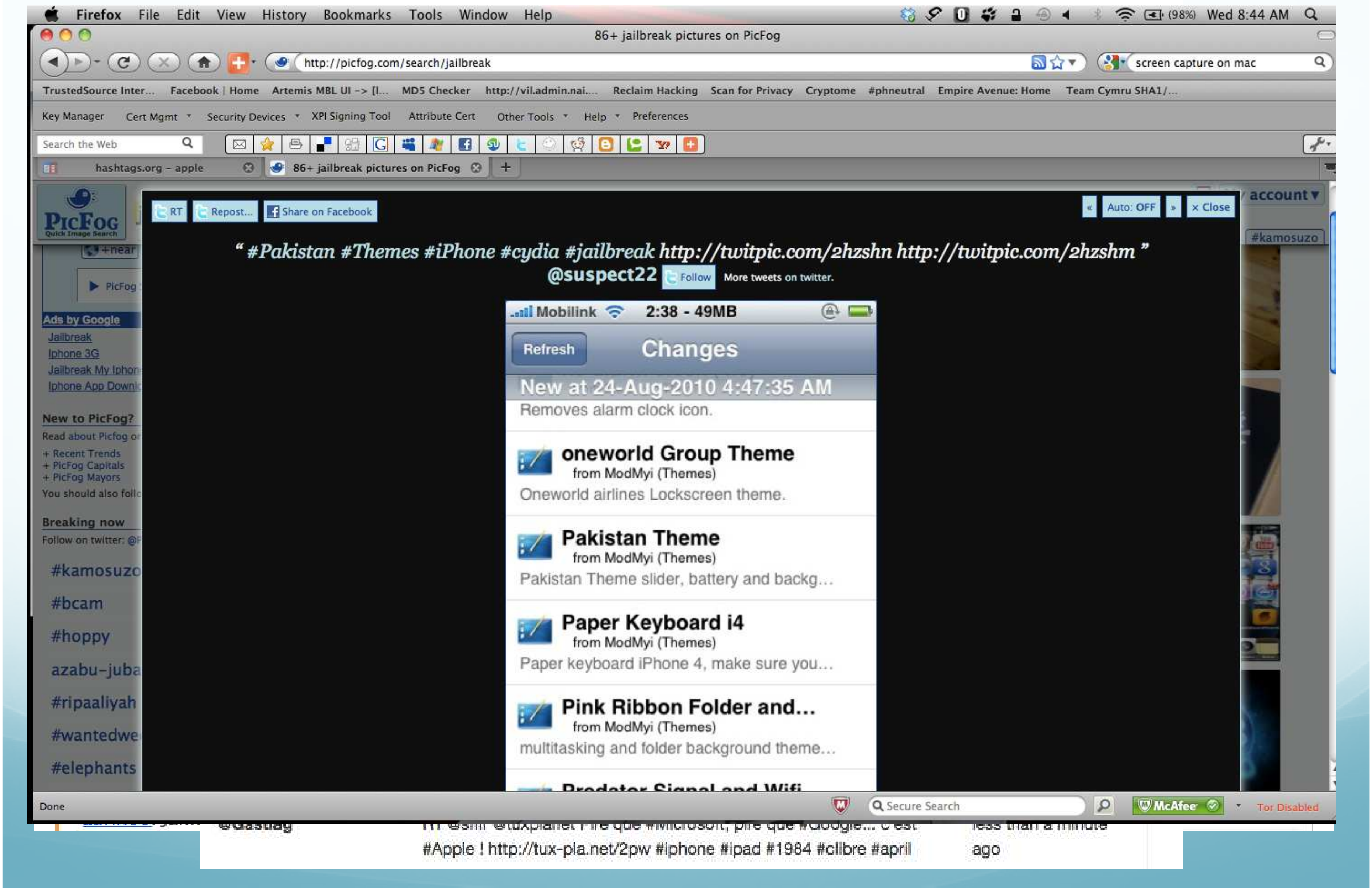
jmecaldwell2
Reading and Praying — at Starbucks http://gowal.la/c/2n2pq?137
48 minutes ago from Gowalla

jmecaldwell2
A sermon about sex, marriage, and much more! The Quest for Radical Holiness: http://wp.me/pZ4Fo-3p
about 19 hours ago from WordPress.com

jmecaldwell2
A quick word from the heart of your pastor - I Will Let You Down: http://wp.me/pZ4Fo-3n
August 23 @ 3:51 PM from WordPress.com

jmecaldwell2
A quick word from the heart of your pastor - I Will Let You Down: http://wp.me/pZ4Fo-3n
August 23 @ 3:51 PM from WordPress.com
More from jmecaldwell2 • Share Tweet

Mining Twitter



“#Pakistan #Themes #iPhone #cydia #jailbreak http://twitpic.com/2hzshn http://twitpic.com/2hzshm”
@suspect22

New at 24-Aug-2010 4:47:35 AM
Removes alarm clock icon.

oneworld Group Theme
from ModMyi (Themes)
Oneworld airlines Lockscreen theme.

Pakistan Theme
from ModMyi (Themes)
Pakistan Theme slider, battery and backg...

Paper Keyboard i4
from ModMyi (Themes)
Paper keyboard iPhone 4, make sure you...

Pink Ribbon Folder and...
from ModMyi (Themes)
multitasking and folder background theme...

Predator Signal and Wifi

@Gastiag RT @sm @tuxplanet Pire que #Microsoft, pire que #Google... c'est #Apple ! http://tux-pla.net/2pw #iphone #ipad #1984 #clibre #april less than a minute ago

Let’s Play A Game…..